

SwilaPass - Bypassing Firewall avec un RPi

“ Si tu veux faire ce tutoriel sur autre chose qu'un rpi, vérifie que le kernel (`uname -r`) est une version au delà de 4.19

J'ai mis à jour ce tutoriel pour fonctionner avec le projet `wg-easy` pour avoir une sympathique interface pour gérer les différents clients du VPN (et aussi simplifier l'installation)

Dans ce tutoriel:

- Configurer un raspberry PI sans écran, clavier ou souris à connecter dessus (headless)
- Ouvrir les ports d'un modem
- Installation de Docker sur un serveur Debian/Raspbian
- Installation de wg-easy sur Docker (wg-easy contient wireguard en plus d'une interface pour y accéder simplement)
- Ajouter et configurer des clients Wireguard sur PC et téléphone

? Matériel requis

- Un ordinateur
- Un raspberry Pi (dans ce cas, un Rpi4)
- Une carte micro SD (et un adaptateur pour l'ordi si besoin)
- Une alimentation pour le raspberry
- Un câble ethernet pour une connection optimale

? Préparation du raspberry

- D'abord il faut installer l'OS de raspberry, dans ce cas ci, on va utiliser [rpi-imager](#) pour l'installer sur la micro SD et on va choisir *Raspberry Pi OS Lite*.

```
yay rpi-imager  
sudo rpi-imager
```

- Dans l'installateur, sélectionne `Raspberry Pi OS Lite` pour l'OS, puis ta carte micro SD, puis va dans les paramètres et configure le.
- Brancher le Raspberry Pi et attendre un peu, ensuite se connecter via SSH: (avec le mot de passe choisi dans l'étape précédente)

```
ssh pi@raspberrypi
```

? Préparation du réseau

- Trouve l'adresse privée de ton raspberry pi

```
hostname -I
```

- Va sur `http://192.168.1.1` et connecte toi (les identifiants sont souvent écrit derrière le modem)
- Va dans la redirection des ports et ajoute la règle suivante:

Protocol	Début du port externe	Fin du port externe	Port interne	Hôte interne	Nom
UDP	53	53	53	<ip locale du raspberry pi>	wireguard

? Installation de Docker

Pour installer docker on peut utiliser les commandes suivantes :

```
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/debian \
$(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt update
sudo apt install docker-ce
sudo systemctl start docker
```

? Installation de wg-easy

Maintenant vous pouvez simplement lancer le bloc de commandes suivant pour automatiquement installer Wireguard (une petite interface web en prime) :

```
read -p "Le mot de passe pour l'administration de votre VPN: " PASSWORD
sudo docker run --name wg-easy -d \
  -e WG_HOST=$(curl ifconfig.me) \
  -e PASSWORD=$PASSWORD \
  -e WG_PORT=53 \
  -e WG_DEFAULT_ADDRESS=192.168.215.x \
  -p 53:51820/udp -p 51821:51821/tcp \
  --restart unless-stopped \
  --cap-add=NET_ADMIN \
  --cap-add=SYS_MODULE \
  --sysctl="net.ipv4.conf.all.src_valid_mark=1" \
  --sysctl="net.ipv4.ip_forward=1" \
  weejewel/wg-easy
```

“ Note: Vous devez juste être sûr qu'il n'y a pas de firewall et si il y en a un, que les ports 53 et 51821 soit accessibles.

“ Je vous invite vivement de transformer cette commande en Docker-Compose comme vu dans [Utiliser Docker Compose](#)

? Configurer les clients

Maintenant il suffit d'installer Wireguard sur son téléphone et son ordi. Puis d'aller sur le lien `http://ADDR_LOCALE_DU_RPI:51821` et se connecter.

Une fois dans le panel, il suffit de cliquer sur "New" puis donner un nom à l'appareil. Ensuite on peut afficher son QR code ou son fichier de configuration qu'il suffit d'ajouter dans l'application.

Sur Linux il faut l'ajouter dans `/etc/wireguard/wg0.conf` en ayant `wireguard-tools` installé. Ensuite on peut lancer `sudo systemctl start wg-quick@wg0` pour démarrer le VPN.

Et c'est tout !